TP : Active Directory (Services Annuaires)

Public(s)	Section de BTS SIO option : SISR
Savoir(s)	C21 Installer et configurer un microordinateur C22 Installer et configurer un réseau
Capacité(s)	C22 Installer et configurer un réseau C26 Installer un routeur
Objectif(s)	• Créer un contrôleur de domaine. • Joindre les PC clients au domaine. • Créer les comptes utilisateurs dans un domaine. • Les mêmes utilisateurs feront parti des groupes adéquats, qui possèdent un profil itinérant, permettant ainsi à ces utilisateurs à se connecter avec leurs profils propres.
Professeur	Christophe CHITTARATH

Un groupe de travail réseau est relativement facile à mettre en place, l'inconvénient est qu'il n'y ait pas de règle commune à tous afin de gérer d'une façon cohérente les tâches d'administration réseau, par exemple les mots de passe, les partages…etc.

Microsoft version serveur dispose un service appelé Active Directory, qui permet de centraliser la gestion de l'administration réseau, et ce à travers des objets tels que les comptes utilisateurs, les profils, GPO (Group Policy Objects) …etc.

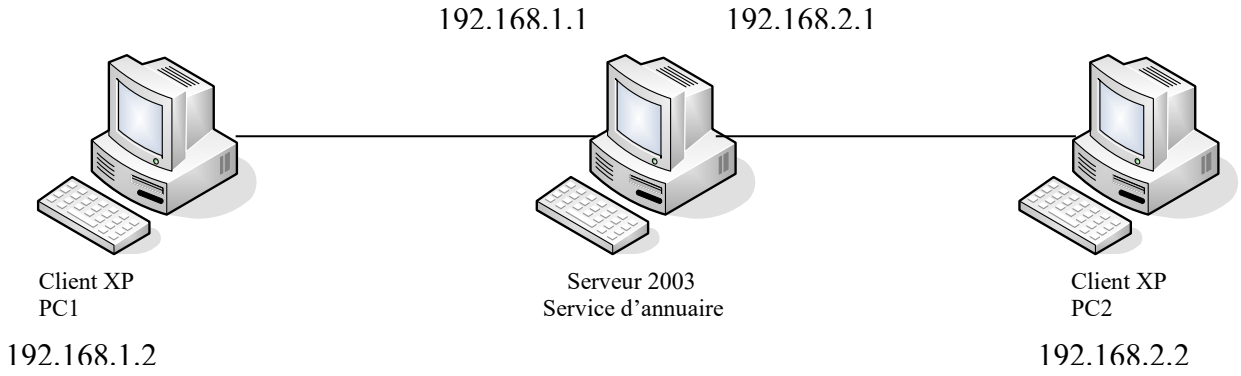
L'installation du service AD promeut un serveur en contrôleur de domaine qui centralise les échanges, les authentifications, les applications des règles prédéfinies au sein du domaine.

Cette PTI consiste à étudier et à mettre en évidence le rôle joué par les profils :

- Défault Users
- All Users
- Local
- Itinérant
- Obligatoire

Elle a pour but de déployer les stratégies de groupe afin de centraliser et optimiser l'administration des objets (machines, compte d'utilisateurs…) dans un domaine.

Configuration du réseau : à compléter les adresses IP



Configuration requise :
Vous créez un team contenant trois postes (1 serveur 2003 et 2 PC client XP)

Configurer vos postes selon le tableau ci-dessous :

Hostname	IP	Masque	Passerelle	DNS
PC1	192.168.1.2	255.255.255.0	192.168.1.1	192.168.1.1
PC2	192.168.2.2	255.255.255.0	192.168.2.1	192.168.2.1
serveur	192.168.1.1	255.255.255.0	néant	127.0.0.1
	192.168.2.1	255.255.255.0		127.0.0.1

Voici le scénario proposé :

Première étapes :

I) Créer et configurer un domaine dans un serveur Microsoft 2003

a) l'utilisation de la commande _____ dans l'invite de commande pour créer un domaine.
b) Valider les options par défaut, proposées par le logiciel.
c) Nom du domaine **lerebours.fr** ; nom NetBios : **lerebours**
d) Service DNS à installer (si ce n'est pas déjà fait)
Démarrer – Panneau de configuration – Ajoute et suppression des composants – Service de mis en réseau - DNS

e) Aller dans **Outils d'administration – Utilisateur et Ordinateur Active Directory**

pour vérifier que le domaine **lerebours.fr** est bien créé.

II) Joindre les PC client au domaine, en faisant

Clic droit sur poste de travail – Propriété – Nom de l'ordinateur - Modifier – Saisir bts.local comme nom du domaine – s'authentifier en tant que l'administrateur du domaine

f) Aller dans **Outils d'administration – Utilisateur et Ordinateur Active Directory – Computer** : Pour vérifier que les PC client font bien parti du domaine lerebours.fr

III) Création des comptes

g) Aller dans le domaine **bts.local**, clic droit pour créer un utilisateur, remplir les champs nécessaires pour la création du compte ; vous utilisez le mot de passe unique Cmsi2026! pour tous les utilisateurs crées (respecter la case).

Vous remarquerez que la stratégie de mot de passe avec complexité est activée.

IV) l'étude des profils
1ère connexion :
- Se connecter au domaine, à partir du PC1, en tant que l'administrateur.
- Aller dans le répertoire c:\Ducuments and Setting
- Constater l'existence de deux répertoires : All Users et Défault Users.
  Si vous ne trouvez pas Défault Users, c'est qu'il est caché ; il faut donc « décacher ».
- Ajouter alluser1.txt dans le sous répertoire Bureau de All Users, et default1.txt dans le sous répertoire Bureau de Default Users.

2ème connexion :
- Se connecter au domaine, à partir du PC1, en tant que l'utilisateur X, pour la première fois.
- Constater que les documents alluser1.txt et default1.txt apparaissent à l'écran (bureau).

3ème connexion :
- Se connecter au domaine, à partir du PC1, en tant que l'administrateur.
- Aller dans le répertoire c:\Ducuments and Setting
- Ajouter **alluser2.txt** dans le sous répertoire **Bureau** de **All Users,** et **default2.txt** dans le sous répertoire **Bureau** de **Default Users.**

4ème connexion :
- Se connecter au domaine, à partir du PC1, en tant que l'utilisateur X, pour la deuxième fois.
- Constater que les documents **alluser1.txt, alluser2.txt** et **default1.txt** apparaissent à l'écran mais pas **default2.txt**

Hypothèse sur Défault Users :

_____

Vérification de l'hypothèse :

5ème connexion :
- Se connecter au domaine, à partir du PC1, en tant que l'utilisateur Y, pour la première fois.
- Constater que les documents **alluser1.txt, alluser2.txt** et **default1.txt et default2.txt** apparaissent à l'écran.

Hypothèse sur All Users : _____

Vérification de l'hypothèse :

Transformer profil local en profil itinérant

6ème connexion : A faire sur le contrôleur du domaine
- Transformer le profil local de l'utilisateur X en profil itinérant.
- Création du profil itinérant :
  a) Créer un dossier sur le bureau appelé **profil**,
  b) Clic droit sur ce dossier – propriété
     Partage - **Tout le monde**. - **Contrôle Total**
     Sécurité - **Tout le monde**. - **Contrôle Total** (à ajouter le groupe ***Tout le monde***)
  c) Créer un sous répertoire au nom de l'utilisateur sous le répertoire **profil.**
  d) Aller dans le compte de l'utilisateur X, choisir l'onglet **Profil**, dans **chemin de profil**, entrer le chemin UNC (Uniform Naming Convention) qui a la forme : \\nom_du_serveur\nom_du partage\%username%
     Pour obtenir le nom du serveur, Dans une fenêtre de DOS taper **hostname**
     Il faut saisir tel quel **%username%**
- Se connecter au domaine, à partir du ***PC1***, créer un dossier dans bureau appelé **test_profil**. Puis vous quittez la session.
- Sur le serveur, on observer dans le dossier **\profil\X** apparition du dossier **test_profil** de l'utilisateur X ;
- Se connecter au domaine, à partir du PC2, observer sur bureau le dossier l'apparition du dossier **test_profil** de l'utilisateur X ;

Conclusion :
On ne voit pas sur PC2, les **AllUsers1.txt** et **AllUsers2.txt** ceci montre que ce profil est local, propre au PC local et il superpose son profil de l'utilisateur.

Transformer un profil Itinérant en profil Obligatoire.
Un profil obligatoire est un profil itinérant, sur lequel on peut effectuer des modifications, mais qui ne seront pas prises en comptes quand l'utilisateur quitte la session. Le profil itinérant permet de conserver l'homogénéité du profil dans le temps ; ceci étant plus important, s'il s'agit d'un profil commun à un group de personnes ; exemple : le profil type créé pour des élèves de différentes classe ; les élèves sont sur de trouver à chaque connexion, le même environnement de travail.

- Aller dans **\profil\X**,
- Modifier l'extension du fichier ntuser.**dat** en ntuser.**man**
- Se connecter au domaine, à partir du PC1, modifier le fond d'écran puis quitter la session.
- Se connecter au domaine, à partir du PC1, constatez que la modification du fond d'écran n'a pas été prise en compte.

GPO Group Policy Object

Stratégie Redirection des dossiers Mes document du profil

- L'inconvénient d'un profil local est que l'utilisateur ne retrouve pas son environnement de travail, lors qu'il change de PC.
- L'avantage d'un profil itinérant est que l'utilisateur retrouve son environnement de travail quelque soit le PC avec lequel il travaille, du moment que le PC en question, fasse parti du domaine.
  Ceci étant, le profil itinérant peut s'enrichir des dossiers avec le temps, et grossit en taille mémoire, par conséquence, le temps de téléchargement du profil du serveur vers le PC devient plus long voire impossible.
- La solution est de créer une stratégie de groupe, qui redirige certains dossiers utilisateur dans le profil vers un dossier appelé par exemple **redirection** indépendant du profil utilisateur. On extrait en quelque sorte, ces dossiers du profil, qui conserve simplement un pointeur dans le profil, assurant la liaison entre ce profil itinérant et les dossiers "retirés" du profil.
  Ainsi, l'utilisateur n'a pas besoin de tout télécharger les dossiers dans son profil itinérant mais simplement quelques éléments de base : papier peint, raccourci... il retrouve cependant les dossiers liés au profil d'une façon transparent grâce au pointeur.

Démonstration

1) Se connecter au nom d'un utilisateur dont le profil est itinérant.
2) Surcharger artificiellement le profil de l'utilisateur, en copiant les fichiers (300 méga octets environ) dans le dossier **Mes documents** du profil de l'utilisateur.
3) Fermer la session. Que constatez-vous ?
4) Se reconnecter de nouveau du même poste. Que constatez-vous ?

Remédiation

Créer un dossier dans la racine appelé par exemple **redirection**, puis le partager avec la permission lecture, écriture, modification…

1) Sous **redirection,** créer un 2ème dossier au nom de l'utilisateur.
2) Création d'une **unité organisatinelle**, appelé **UO1,** pour ce faire, aller dans **Outil administration, utilisateur_active Directory, clic droit sur le nom du domaine…etc**
3) Placer l'utilisateur en question dans **UO1**.
4) Clic droit sur l'**UO1**, **propriété**, puis **stratégie de groupes**, donner un nom à votre stratégie comme par exemple **stratégie_redirection**, puis cliquer sur **modifier.**

5) Développer onglet **Configuration Utilisateur**, puis **Paramètre de Windows,** puis **Redirection du dossier.**
6) Cliquez droit sur **Mes Documents,** choisir **propriété.**
7) Dans Paramètre, choisir **De base – Rediriger les dossiers….**
8) Dans emplacement du dossier cible, choisir **Créer un dossier pour un utilisateur….**
9) Dans Chemin d'accès de la racine : saisir le chemin UNC **\\nom_du_serveur\redirection**
10) Pour actualiser la stratégie de groupe aller dans une fenêtre de DOS, puis taper **gpupdate/force** puis valider.
11) Tester la stratégie en se connectant puis déconnectant au nom de cet utilisateur.
12) Que constatez-vous au niveau du temps de connexion – déconnexion ?
13) Que trouvez-vous dans le sous dossier **Redirection** ?

A tester les autres stratégies :

- **Interdire l'utilisation de l'invite de commande**
  Configuration utilisateur - Modèle d'administration – Système

- **Empêcher l'Accès au panneau de configuration**
  Configuration utilisateur - Modèle d'administration – Panneau de configuration

- **Masquer les lecteurs logiques : A, B , C…etc**
  Configuration utilisateur - Modèle d'administration – Explorateur Windows - Dans poste de travail masquer… ;

- **Créer une sous unité** organisationnelle **UO2**, placer les nouveaux utilisateurs puis montrer que les stratégies activées dans **UO1** (parent) hérite sur UO2.

- **Démontrer que les utilisateur de UO2 peut bloquer l'héritage venant de UO1 (c'est-à-dire de ne pas subir stratégie de parent).**

- **Imaginer une situation conflictuelle** dans l'application d'une stratégie au niveau d'un utilisateur. Démontrer la logique dans l'application de celles-ci dans une telle situation.

A) – Créer un compte toto puis le placer dans UO_A
– Créer un compte titi dans UO_B qui se trouve en dessous de UO_A
- Appliquer la stratégie qui autorise l'accès à l'invite de commande sur OU_A
- Appliquer la stratégie qui refuse l'accès l'invite de commande sur OU_B

Question :
- titi peut-il accéder à l'invite de commande et pourquoi ?

B) Stratégie par rapport au groupe
Créer un compte tutu dans le conteneur USER, créer une UO_C à la racine
Créer un groupe C dans UO_C, déclarer l'appartenance de titi et tutu dans le groupe C.
- Appliquer la stratégie qui refuse l'accès au panneau de configuration sur UO_C
- Appliquer la stratégie qui refuse l'accès au panneau de configuration sur UO_B

Question :
- titi et tutu peuvent-ils accéder au panneau de configuration et pourquoi ?

C) stratégie plus haute ou plus basse:
- Appliquer une deuxième stratégie qui autorise l'accès au panneau de configuration sur UO_C.

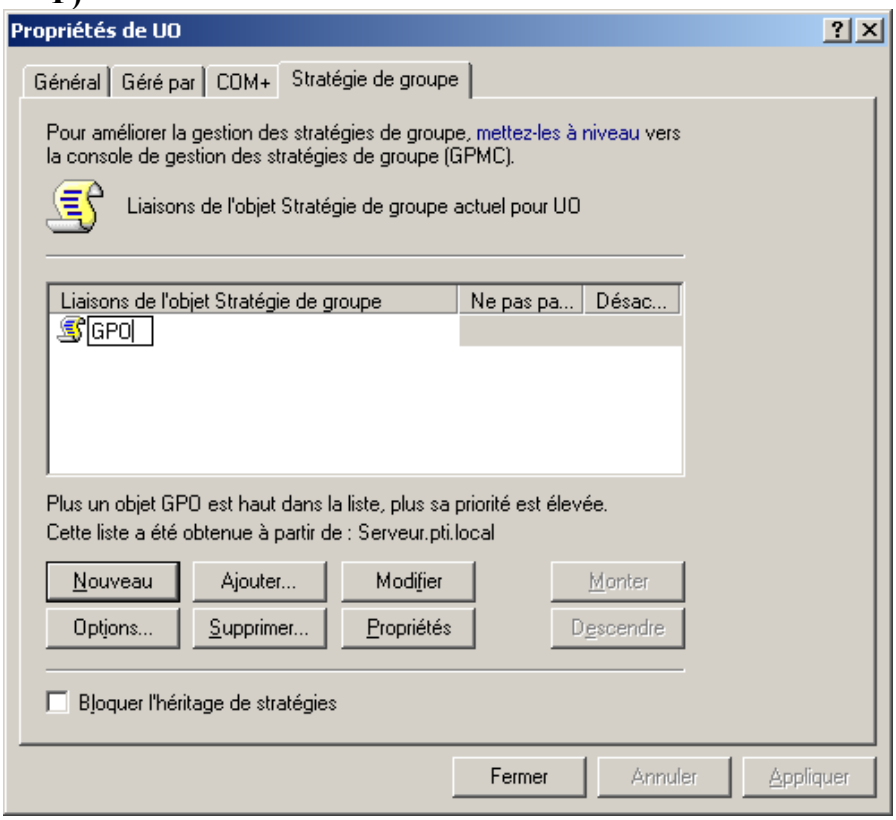
Question
- tutu peut-il accéder au panneau de configuration et pourquoi ?

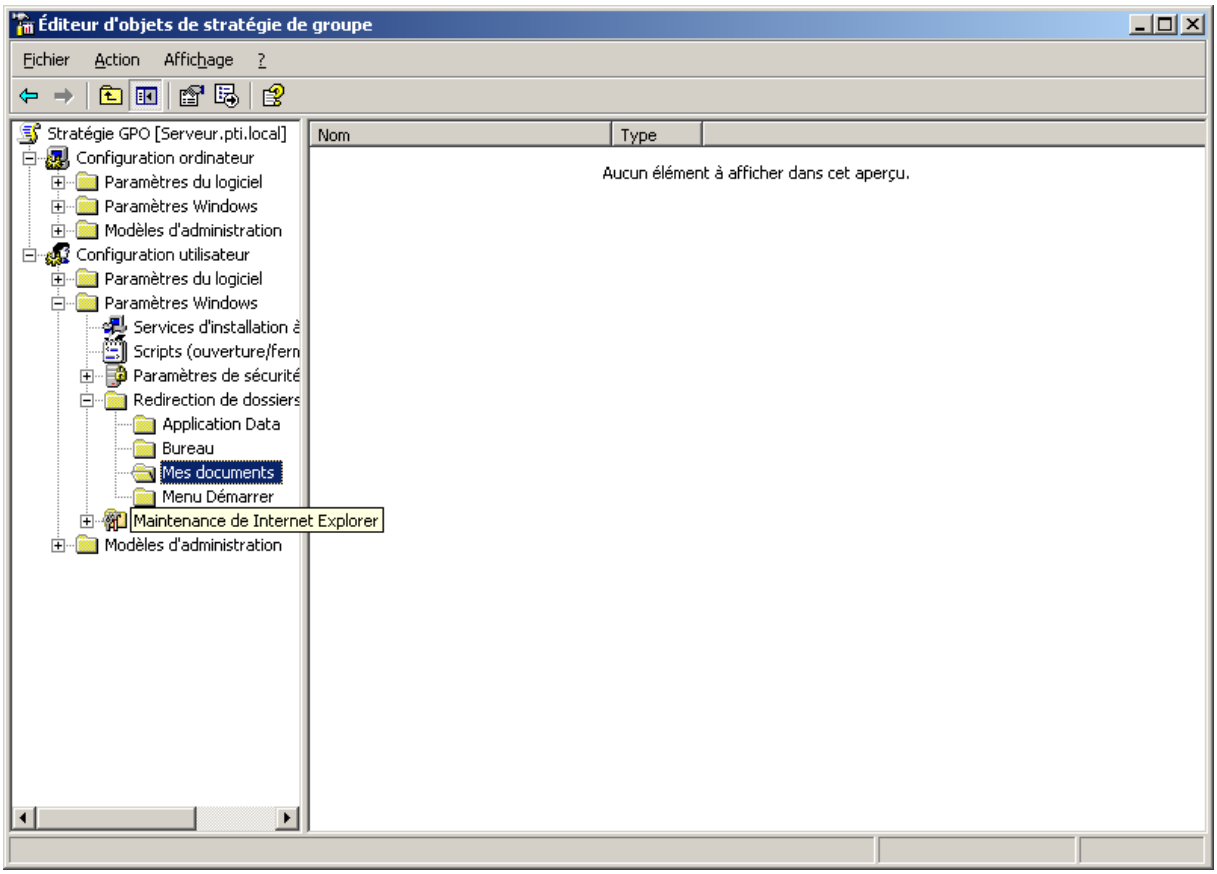
Permuter les deux stratégies, que constatez-vous ? Conclusion.

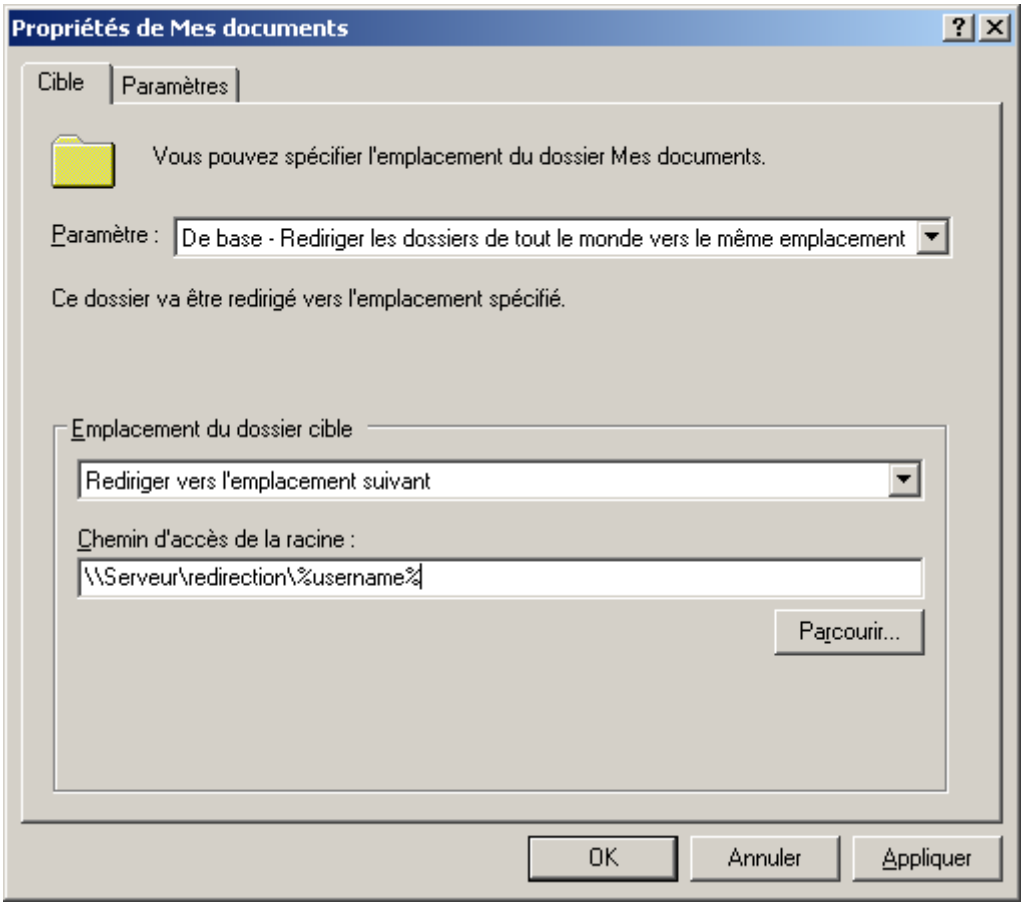
D) stratégie la plus restrictive
En cas de conflit de stratégie entre deux groupes dans deux U.O différentes, laquelle des deux stratégies emporte sur l'autre.

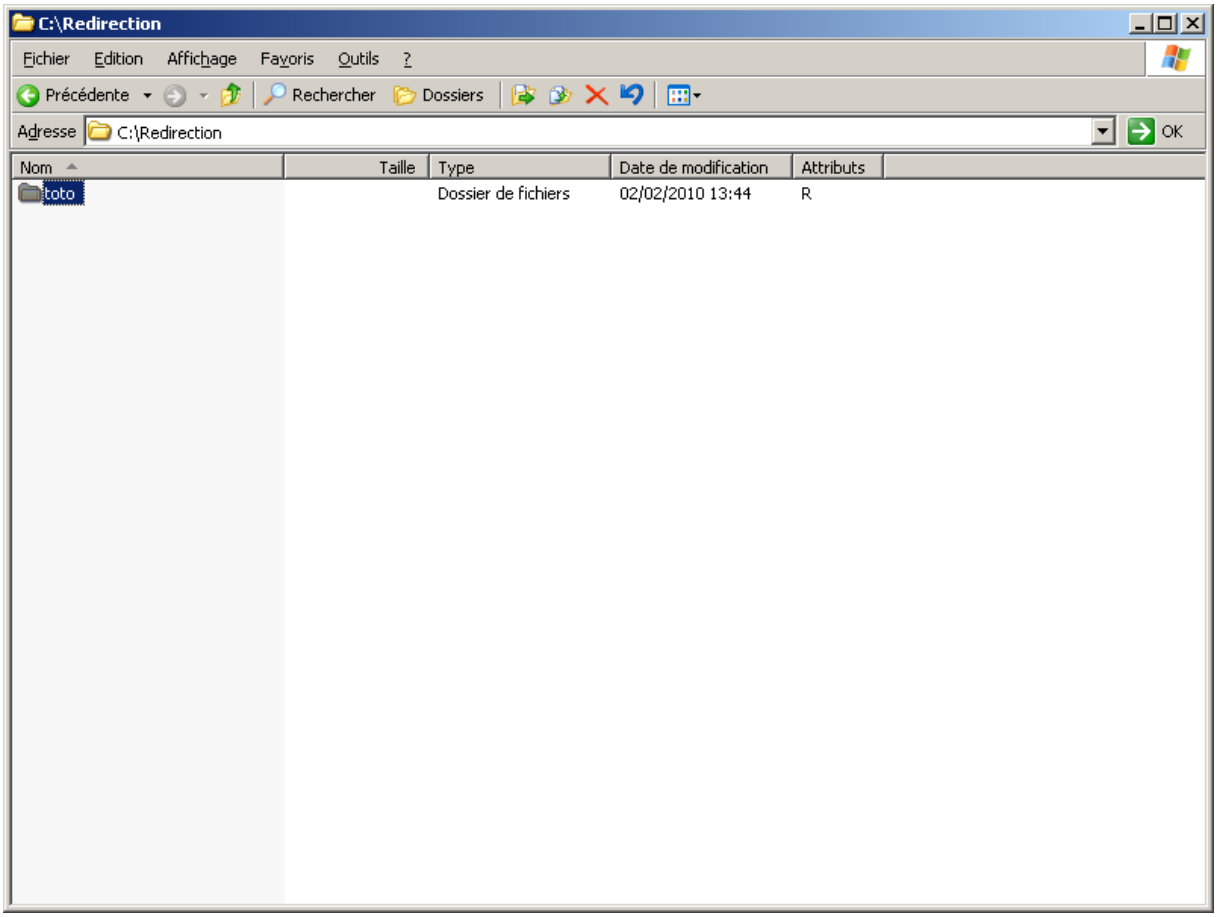
E) par rapport au poste
En cas de conflit de stratégie entre celle s'applique sur le poste, et celle qui s'applique sur un compte utilisateur, laquelle des deux stratégies emporte sur l'autre.

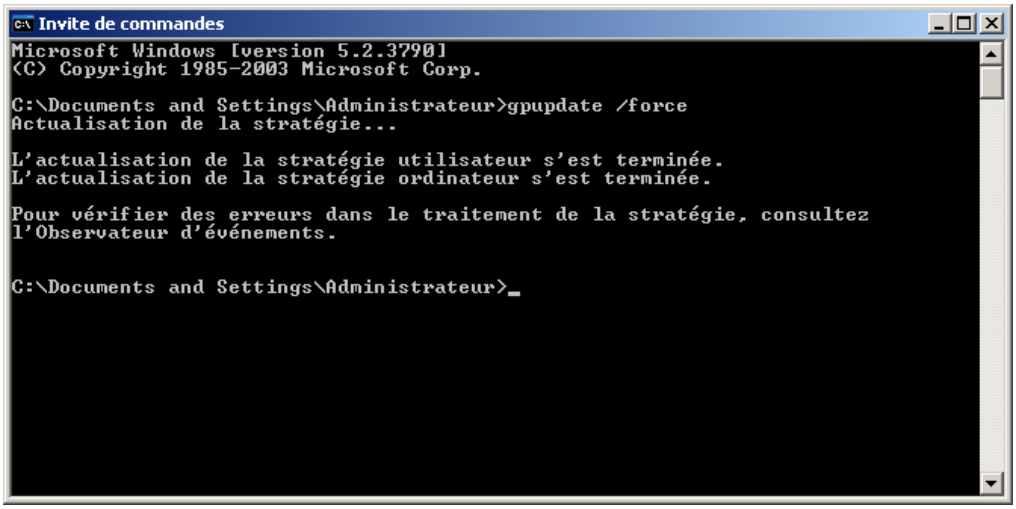
F)

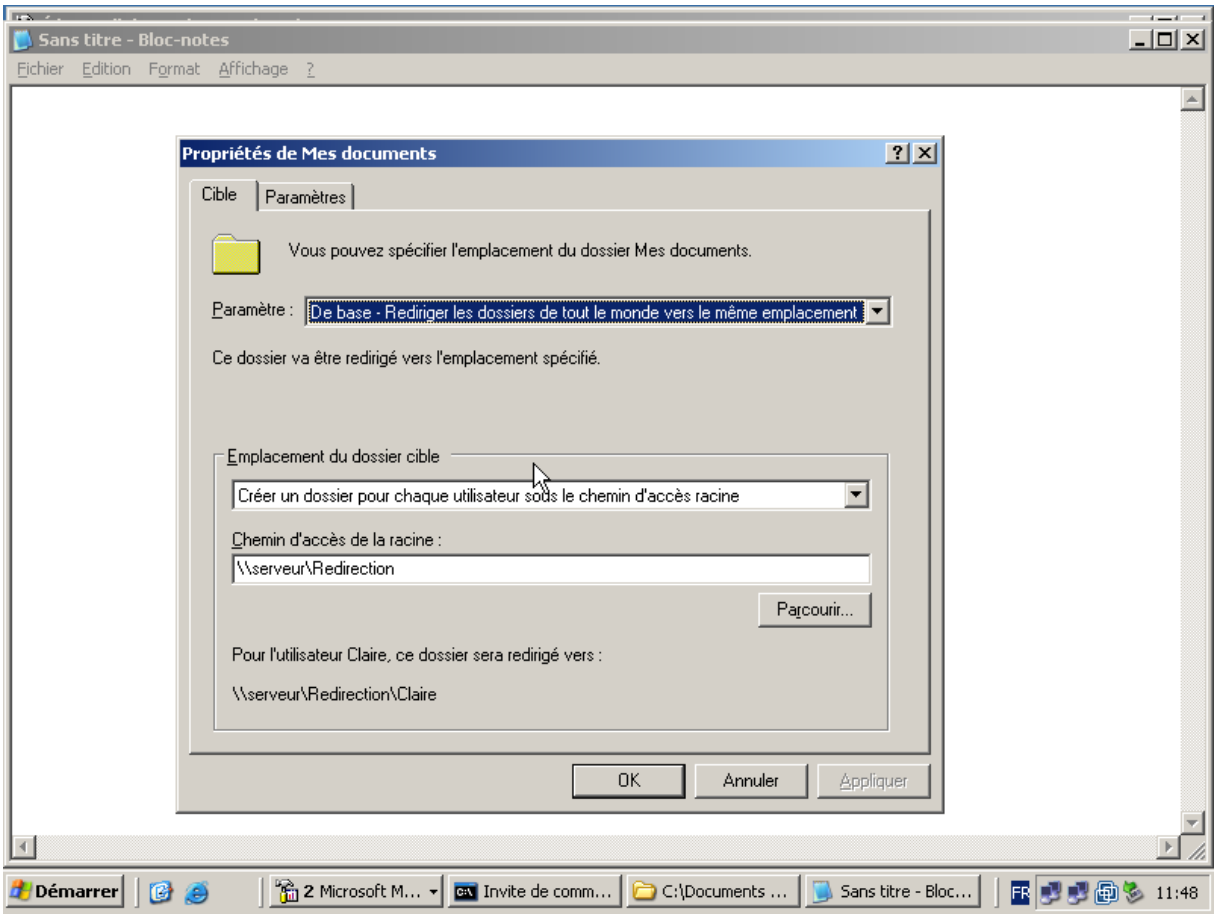

Propriétés de UO
Général
Géré par
COM+
Stratégie de groupe
Pour améliorer la gestion des stratégies de groupe, mettez-les à niveau vers la console de gestion des stratégies de groupe (GPMC).
Liaisons de l'objet Stratégie de groupe actuel pour UO
Liaisons de l'objet Stratégie de groupe
Ne pas pa...
Désac...
GPO
Plus un objet GPO est haut dans la liste, plus sa priorité est élevée.
Cette liste a été obtenue à partir de : Serveur.pti.local
Nouveau
Ajouter...
Modifier
Monter
Options...
Supprimer...
Propriétés
Descendre
Bloquer l'héritage de stratégies
Fermer
Annuler
Appliquer


Éditeur d'objets de stratégie de groupe
Fichier
Action
Affichage
?
Stratégie GPO [Serveur.pti.local]
Configuration ordinateur
Paramètres du logiciel
Paramètres Windows
Modèles d'administration
Configuration utilisateur
Paramètres du logiciel
Paramètres Windows
Services d'installation à
Scripts (ouverture/fern
Paramètres de sécurité
Redirection de dossiers
Application Data
Bureau
Mes documents
Menu Démarrer
Maintenance de Internet Explorer
Modèles d'administration
Nom
Type
Aucun élément à afficher dans cet aperçu.


Propriétés de Mes documents
Cible
Paramètres
Vous pouvez spécifier l'emplacement du dossier Mes documents.
Paramètre :
De base - Rediriger les dossiers de tout le monde vers le même emplacement
Ce dossier va être redirigé vers l'emplacement spécifié.
Emplacement du dossier cible
Rediriger vers l'emplacement suivant
Chemin d'accès de la racine :
\\Serveur\redirection\%username%
Parcourir...
OK
Annuler
Appliquer


C:\Redirection
Fichier
Edition
Affichage
Favoris
Outils
?
Précédente
Rechercher
Dossiers
Adresse
C:\Redirection
OK
Nom
Taille
Type
Date de modification
Attributs
toto
Dossier de fichiers
02/02/2010 13:44
R


Invite de commandes
Microsoft Windows [version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrateur>gpupdate /force
Actualisation de la stratégie...
L'actualisation de la stratégie utilisateur s'est terminée.
L'actualisation de la stratégie ordinateur s'est terminée.
Pour vérifier des erreurs dans le traitement de la stratégie, consultez
l'Observateur d'événements.
C:\Documents and Settings\Administrateur>_


Sans titre - Bloc-notes
Fichier Edition Format Affichage ?
Propriétés de Mes documents
Cible
Paramètres
Vous pouvez spécifier l'emplacement du dossier Mes documents.
Paramètre :
De base - Rediriger les dossiers de tout le monde vers le même emplacement
Ce dossier va être redirigé vers l'emplacement spécifié.
Emplacement du dossier cible
Créer un dossier pour chaque utilisateur sous le chemin d'accès racine
Chemin d'accès de la racine :
\\serveur\Redirection
Parcourir...
Pour l'utilisateur Claire, ce dossier sera redirigé vers :
\\serveur\Redirection\Claire
OK
Annuler
Appliquer
Démarrer
2 Microsoft M...
Invite de comm...
C:\Documents ...
Sans titre - Bloc...
FR
11:48